UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,809	01/30/2002	Avner Halperin	1117-US	3173

24505 7590 07/07/2005

DANIEL J SWIRSKY
PO BOX 2345
BEIT SHEMESH, 99544
ISRAEL

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,809	HALPERIN ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of Continuing Application priority date under 35 U.S.C. 120 is acknowledged.

The application is filed on 1/30/2002 but is a Continuation-In-Part of Application number 09/993,591 filed on 11/27/2001 and has a U.S. provisional application number 60/298,390 filed on 6/18/2001.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 37 and 38 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 132 of copending Application No. 09/993,591. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

3. Claim 49 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 27 of copending Application No. 09/993,591. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

4. Claim 50 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 13 of copending Application No. 09/993,591. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

5. Claim 51 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 132 of copending Application No. 09/993,591. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> **A person shall be entitled to a patent unless –**
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 – 5, 7, 9, 11 – 14, 22 – 29, 49 and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Tarbotton (Patent Number: 6757830).

As per claim 3, Tarbotton teaches a method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups (Tarbotton: Column 5 Line 30 – 32);

identifying a known malicious software behavior pattern for any of said groups (Tarbotton: Column 14 Line 9 – 23);

determining a normal behavior pattern for any of said groups (Tarbotton: Column 14 Line 9 – 23);

setting a threshold between said normal and malicious software behavior patterns (Tarbotton: Column 14 Line 9 – 23); and

detecting behavior is detected that exceeds said threshold (Tarbotton: Column 3 Line 15 – 35).

As per claim 7, Tarbotton teaches a method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups (Tarbotton: Column 5 Line 30 – 32);

identifying activity suspected of being malicious occurring sequentially in at least two of said groups between which a proximity measure is defined (Tarbotton: Column 3 Line 40 – 46); and

searching for communication events between said at least two groups which are associated with the progress of malicious software from the first of said at least two groups to the second of said at least two groups (Tarbotton: Column 3 Line 36 – 65).

As per claim 22 and 50, Tarbotton teaches a method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups (Tarbotton: Column 5 Line 30 – 32);

receiving messages sent from any of said computing devices (Tarbotton: Column 3 Line 36 – 65);

buffering any of said messages received from any of said computing devices in one of said groups and destined for any of said computing devices in a different one of said groups for a predetermined delay period prior to forwarding said messages to their intended recipients (Tarbotton: Column 3 Line 36 – 65).

As per claim 1, 9 and 49, the claim limitations are met as the same reasons set forth in claim 3.

As per claim 2, Tarbotton further teaches said measuring step comprises measuring a ratio of the number of messages sent within any of said groups and between any of said groups over a period of time (Tarbotton: Column 3 Line 25 – 29).

As per claim 4, Tarbotton further teaches performing a malicious software containment action if behavior is detected that exceeds said threshold (Tarbotton: Column 4 Line 27 – 45).

As per claim 5, Tarbotton further teaches any of said patterns are expressed as any of a numbers of message per unit of time, a shape of a utilization graph, a graph of e-mail messages per unit of time, a histogram of communication frequency vs. proximity measure, a number of messages sent within any of said groups, number of messages sent from one of said groups to a another one of said groups, and a histogram of e-mail lengths (Tarbotton: Column 14 Line 9 – 23).

As per claim 11, Tarbotton further teaches performing at least one malicious software containment action upon determining that said correlated target behavior information corresponds to a predefined suspicious behavior pattern (Tarbotton: Column 4 Line 27 – 45).

As per claim 12 and 27, Tarbotton further teaches said grouping step comprises grouping according to a measure of proximity (Tarbotton: Column 14 Line 9 – 23).

As per claim 13 and 28, Tarbotton further teaches said measure of proximity is a measure of logical proximity (Tarbotton: Column 14 Line 9 – 23).

As per claim 14 and 29, Tarbotton further teaches said measure of logical proximity is a frequency of communication between at least two computing devices (Tarbotton: Column 14 Line 9 – 23).

As per claim 23, Tarbotton further teaches said delay period is dynamic (Tarbotton: Column 3 Line 15 – 35).

As per claim 24, Tarbotton further teaches said delay period is adjustable according to a level of suspicious behavior in any of said groups (Tarbotton: Column 3 Line 15 – 35).

As per claim 25, Tarbotton further teaches said buffering step comprises separately buffering messages sent within any of said groups and messages sent outside of any of said groups (Tarbotton: Column 3 Line 36 – 65).

As per claim 26, Tarbotton further teaches performing at least one malicious software containment action upon said buffer (Tarbotton: Column 4 Line 27 – 45).

7. Claim 8 is rejected under 35 U.S.C. 102(e) as being anticipated by Burrows (Patent Number: 2002/0073338).

As per claim 8, Burrows teaches a method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups (Burrows (provisional): Page 3, 1st Para);

identifying generally simultaneously suspicious malicious activity in at least two of said groups between which a proximity measure is defined (Burrows (provisional): Page 4, 3rd Para & Page 6, 4th Para); and

identifying a generally similar communication received by said groups (Burrows (provisional): Page 4, 3rd Para & Page 6, 4th Para).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 6, 15 – 21, 30 – 36, 37 – 45 and 46 – 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarbotton (Patent Number: 6757830), in view of Burrows (Patent Number: 2002/0073338).

As per claim 37, Tarbotton teaches a method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups (Tarbotton: Column 5 Line 30 – 32);

configuring each of said groups to maintain a malicious software detection sensitivity level (Tarbotton: Column 14 Line 9 – 23); and

Tarbotton does not disclose expressly upon detecting suspected malicious software activity within any of said groups, notifying any other of said groups of said detected suspected malicious software activity.

Burrows teaches upon detecting suspected malicious software activity within any of said groups, notifying any other of said groups of said detected suspected malicious software activity (Burrows (provisional): Page 3, 3rd Para, Line 6).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Burrows within the system of Tarbotton because (a) Tarbotton discloses network unwanted property such as high message ratio in terms of message / sec (Tarbotton: Column 14 Line 9 – 23) and (b) Burrows teaches monitoring / detecting any network undesirable behavior pattern sent by a host and isolate them from the rest of the hosts in the network, or at least from the subnet they are disrupting (Burrows: Page 2, 3rd Para & 2nd Para).

As per claim 6, Tarbotton does not disclose expressly notifying at least one neighboring group of said group in which said threshold is exceeded.

Burrows teaches notifying at least one neighboring group of said group in which said threshold is exceeded (Tarbotton: Column 14 Line 9 – 23 & Burrows (provisional): Page 3, 3rd Para, Line 6). See the same rationale of combination applied herein as above in rejecting claim 37.

As per claim 15, 18, 30 and 33, Tarbotton does not disclose expressly said grouping step comprises applying a clustering algorithm to said measure of logical proximity.

Burrows teaches said grouping step comprises applying a clustering algorithm to said measure of logical proximity (Burrows (provisional): Page 6, 2nd Para: Topology Discovery). See the same rationale of combination applied herein as above in rejecting claim 37.

As per claim 16 and 31, Tarbotton does not disclose expressly replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group.

Burrows further teaches replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group (Burrows (provisional): Page 3, 3rd Para: using a uniform packet monitoring tool). See the same rationale of combination applied herein as above in rejecting claim 37.

As per claim 17 and 32, Tarbotton does not disclose expressly identifying a plurality of neighboring ones of said groups.

Burrows further teaches identifying a plurality of neighboring ones of said groups (Burrows (provisional): Page 6, 2nd Para: Topology Discovery). See the same rationale of combination applied herein as above in rejecting claim 37.

As per claim 19, 34 and 46, Burrows teaches upon detecting suspect malicious software activity in any of said groups, notifying any of said neighboring groups of said suspect malicious software activity (Burrows (provisional): Page 3, 3rd Para).

As per claim 20, 35 and 47, Burrows teaches any of said neighboring groups using, in response to said notification, the same sensing mechanisms as said group

from which said notification was received (Burrows (provisional): Page 3, 3rd Para: using a uniform packet monitoring tool).

As per claim 21 and 36, Tarbotton does not disclose expressly any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors.

Burrows further teaches any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors (Burrows (provisional): Page 3, 3rd Para: using a uniform packet monitoring tool). See the same rationale of combination applied herein as above in rejecting claim 37.

As per claim 38, Tarbotton further teaches adjusting said malicious software detection sensitivity level at any of said notified groups according to a predefined plan (Tarbotton: Column 3 Line 35 – 65).

As per claim 39, Tarbotton further teaches said grouping step comprises grouping according to a measure of proximity (Tarbotton: Column 14 Line 9 – 23).

As per claim 40, Tarbotton further teaches said measure of proximity is a measure of logical proximity (Tarbotton: Column 14 Line 9 – 23).

As per claim 41, Tarbotton further teaches said measure of logical proximity is a frequency of communication between at least two computing devices (Tarbotton: Column 14 Line 9 – 23).

As per claim 42 and 45, Burrows further teaches said grouping step comprises applying a clustering algorithm to said measure of logical proximity (Burrows (provisional): Page 6, 2nd Para: Topology Discovery).

As per claim 43, Burrows further teaches replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group (Burrows (provisional): Page 3, 3rd Para: using a uniform packet monitoring tool).

As per claim 44, Burrows further teaches identifying a plurality of neighboring ones of said groups (Burrows (provisional): Page 6, 2nd Para: Topology Discovery).

As per claim 48, Burrows further teaches any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors (Burrows (provisional): Page 3, 3rd Para: using a uniform packet monitoring tool).

9. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tarbotton (Patent Number: 6757830), in view of Shieh (Patent Number: 5278901).

As per claim 10, Tarbotton does not disclose expressly said grouping step comprises grouping such that malicious software will spread according to a predefined spread pattern relative to said groups.

Shieh teaches said grouping step comprises grouping such that malicious software will spread according to a predefined spread pattern relative to said groups (Shieh: Column 17 Line 33 – 39 and Column 2 Line 27 – 29).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shieh within the system of Tarbotton because Shieh teaches providing a pattern-oriented intrusion detection system that detects the intrusions caused by execution of foreign programs containing virus as well as detects the existence of viruses by detecting virus-propagation patterns so that virus activity can be easily tracked and controlled (Shieh: Column 2 Line 14 – 29 and Column 17 Line 33 – 39).

10. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chefalas (Patent Number: 2002/0116639), and in view of Thacker (Patent Number: 2002/0035696).

As per claim 51, Chefalas teaches a method for malicious software detection, the method comprising:

providing multiple pluralities of computers, each plurality of computers being in communication with at least one of said servers (Chefalas: Abstract Line 1 – 6);

detecting suspected virus activity at any of said plurality of computers, and notifying any of said servers of said detected suspected virus activity (Chefalas: Abstract Line 1 – 6).

Chefalas does not teach configuring each a plurality of servers to maintain a virus detection sensitivity level.

Thacker teaches configuring each a plurality of servers to maintain a virus detection sensitivity level (Thacker: Paragraph [0014]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Thacker within the system of Chefalas because Thacker teaches a new and improved system for effectively protecting computers from viruses that would otherwise require too much time and action on the part of user and many times the protection is too late to prevent infection by using existing virus protection software (Thacker: Paragraph [0004]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100